

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2003 年 12 月 18 日 (18.12.2003)

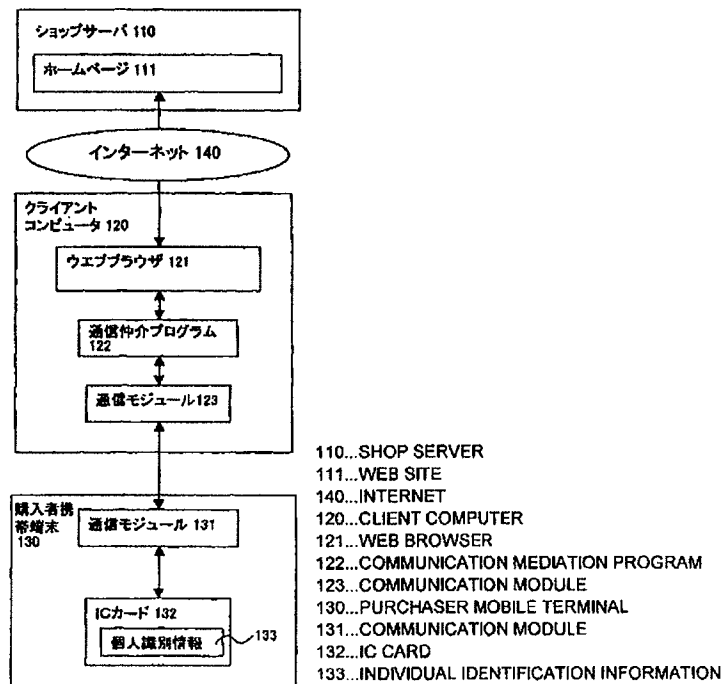
PCT

(10) 国際公開番号
WO 03/105037 A1

- (51) 国際特許分類: G06F 17/60 市 大字大丸1405番地 株式会社富士通パソコンシス
テムズ内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP02/05582
- (22) 国際出願日: 2002 年 6 月 6 日 (06.06.2002) (74) 代理人: 土井 健二, 外(DOI,Kenji et al.); 〒222-0033
神奈川県 横浜市港北区 新横浜3-9-5 第三東昇ビル
林・土井国際特許事務所 Kanagawa (JP).
- (25) 国際出願の言語: 日本語 (81) 指定国 (国内): JP, US.
- (26) 国際公開の言語: 日本語 (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (71) 出願人 (米国を除く全ての指定国について): 富士通
株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神
奈川県 川崎市中原区 上小田中4丁目1番1号 Kanagawa
(JP). 添付公開書類:
— 国際調査報告書
- (72) 発明者; および 2文字コード及び他の略語については、定期発行される
(75) 発明者/出願人 (米国についてのみ): 三浦 正之 各PCTガゼットの巻頭に掲載されている「コードと略語
(MIURA,Masayuki) [JP/JP]; 〒206-0801 東京都 稲城 のガイダンスノート」を参照。

(54) Title: DATA COMMUNICATION MEDIATION APPARATUS COOPERATING WITH PURCHASER MOBILE TERMINAL

(54) 発明の名称: 購入者携帯端末と共働するデータ通信仲介装置



(57) Abstract: In the Internet shopping, user-friendly and secure authentication is realized. A client computer (120) is an ordinary personal computer and has a communication medication program (122) activated when paying out in the shopping. A purchaser mobile terminal (130) is, for example, an IC card-equipped mobile telephone which

[続葉有]



is connected to the client computer by radio or the like. The IC card (132) has a crypt processing function and contains electronic certificate and credit card information. When paying out, the communication mediation program, for authentication, receives an electronic certificate from the IC card and transmits it directly to a shop server (110) without leaving it in a local hard disc.

(57) 要約:

インターネット・ショッピングにおいて使い良さとともによりセキュアな認証を実現する。クライアントコンピュータ(120)は、通常のパーソナルコンピュータであり、ショッピングでの支払いのときに起動する通信仲介プログラム(122)をもつ。購入者携帯端末(130)は、たとえばICカードつき携帯電話であり、クライアントコンピュータと無線などにより接続される。ICカード(132)は、暗号処理能力をもち、あらかじめ電子証明書やクレジットカード情報をストアしている。支払いのとき、通信仲介プログラムは認証のためにICカードから電子証明書を受け取ってそれをローカルのハードディスクに残したりせずに直接ショッピングサーバ(110)に送る。

明細書

5

購入者携帯端末と共働するデータ通信仲介装置

〔技術分野〕

本発明は、認証処理に関し、特にインターネットショッピングにおける個人認証および決済認証処理のデータ通信を仲介するデータ通信仲介プログラムおよび
10 前記データ通信を仲介する通信仲介装置を有するクライアントコンピュータに関する。

〔背景技術〕

インターネット上に作成されている、個人、法人等のホームページから商品や
15 サービス等のアイテムを購入し、代金支払いの決済手続きを行う一連の行為はインターネットショッピングとして現在広く行われている。本明細書では、サービスを購入者が選択可能な商品の1つとみなし、商品やサービス等のアイテムを簡単のために商品として説明する。

購入者はまずインターネットに接続されたパーソナルコンピュータ（以下 PC
20 と略す）などのクライアントコンピュータから、ウェブブラウザを利用しショップのホームページに掲載された商品を開覧し、購入する商品を選択する。購入する商品が決定したら、その旨を告げ購入手続きに入る。この購入手続きにおいて、購入者の身元を明らかにし、本当に取引を行う意思があるかを確認するための個人認証と、購入者によって支払いが行われたか、もしくは購入者に支払能力があるかを確認する決済認証が行われる。個人認証は、購入者個人を特定するための
25 情報である個人情報に基づき行われ、決済認証は、クレジットカード番号や銀行口座番号などの決済情報を基にして行われる。本明細書では、以後個人情報と決済情報を併せて個人識別情報と呼ぶ。ショップは、上記個人認証、決済認証の結果が良好なら、商品を出荷し、こうして購入手続きは終了する。

このようにインターネットショッピングにおいては、個人識別情報が重要な役割を担っている。

- しかしながら、購入者は通常、インターネットショッピングをP Cなどのクライアントコンピュータで行う場合、個人認証や決済認証が必要な場面において、
- 5 クライアントコンピュータ上で個人識別情報を入力している。一般にP Cなどのクライアントコンピュータでは入力された個人識別情報がハードディスクに格納されるため、悪意を持った第三者がハードディスクの情報を直接読み出したり、ネットワークを介して端末装置に侵入して情報を読み出したり、本人が端末装置を離れている間に残っている履歴を盗み見したりして、アカウント、パスワード、
- 10 クレジットカード番号、住所、電話番号、といった個人識別情報が購入者以外の第三者に簡単に漏洩してしまう。その結果、第三者が本人になりすまして商品の購入をする、「なりすまし」が起きる危険性がある。

- 一方、購入者が携帯電話を含めた通信機能を備えた購入者携帯端末でインターネットショッピングを行うこともある。この場合、個人識別情報などのデータは
- 15 ハードディスクのような取り出し可能な独立した装置に格納されるのではなく、購入者携帯端末内部のメモリに格納されるため、P Cなどのクライアントコンピュータと比較すると個人識別情報の漏洩による「なりすまし」が起きる可能性は低い。だが、購入者携帯端末の画面は一般に小さいため、購入者は商品の選択や比較をするために、画面の切り替えやスクロールなどをしなければならず、手間
- 20 がかかり、また PC 等と比較すると通信速度が遅い場合が多く、画像などのデータをダウンロードするのに時間がかかり、通信料金が高い、等の理由から、購買を決定するのに十分な情報が得にくい課題がある。

- したがって、購入者による商品の閲覧には、一画面に複数の画像が表示でき、その詳細な説明が得られるだけの大きさを備えた画面と高速な通信機能を備え、
- 25 購買の決定に十分な情報が得られるクライアントコンピュータを使用し、但し、クライアントコンピュータのハードディスクのような第三者にデータが漏洩する可能性のある場所に個人識別情報が格納されず、結果「なりすまし」を防止できる個人認証、決済認証処理が必要である。

[発明の開示]

本発明の目的は、インターネットショッピングにおいて、画面が大きく、操作性のよいPCなどのクライアントコンピュータを使用して、商品の選択を行いながら、個人認証、決済認証の際要求される個人識別情報をクライアントコンピュータから獲得するのではなく、より情報が第三者に漏洩しにくい購入者携帯端末から獲得し、「なりすまし」を防止する個人認証、決済認証処理を行うことができる環境を提供することにある。

上記目的を達成するために、サーバにコンピュータネットワークを介して接続可能なクライアントコンピュータに、個人識別情報が格納された購入者携帯端末と共働して、個人識別処理を実行させる通信仲介プログラムにおいて、前記個人識別処理は、前記サーバからの個人識別情報要求信号に応答して、当該個人識別情報要求信号を前記購入者携帯端末に転送する手順と、前記購入者携帯端末に格納される前記個人識別情報であって、前記購入者携帯端末が前記個人識別情報要求信号に応答して前記クライアントコンピュータに送信する前記個人識別情報を、前記サーバに転送する手順とを有することを特徴とするプログラムを提供する。

上記発明によれば、大きな画面でより鮮明かつ詳細な情報が得られ、操作性も良好なPCなどのクライアントコンピュータを利用して商品の閲覧、選択が行われ、第三者に個人識別情報が漏洩する可能性がPCなどの端末装置より低い、購入者携帯端末に格納された個人識別情報で個人認証、決済認証が行われることで、「なりすまし」を防止することができる。

[図面の簡単な説明]

- 図1は、本発明の実施例における構成例を示す図である。
- 図2は、電子署名入りデータの信頼性確認の例を示す図である。
- 図3は、第一の実施例でのフローチャートである。
- 図4、5は、第二の実施例でのフローチャートである。
- 図6、7、8、9は、第三の実施例でのフローチャートである。

[発明を実施するための最良の形態]

以下、本発明の実施例について図面に従って説明する。しかしながら、本発明の技術的範囲はかかる実施例によって限定されるものではなく、特許請求の範囲に記載された発明とその均等物に及ぶものである。

図1は、本発明の実施例における構成例を示す図である。

- 5 ショップサーバ110は、ショップのホームページ111を提供するサーバである。クライアントコンピュータ120には、前記ホームページを閲覧するためのウェブブラウザ121と本発明の通信仲介プログラム122とがインストールされ、更に通信モジュール123が備えられている。ウェブブラウザ121と通信仲介プログラム122は同じオペレーティングシステム上で実装されており、
- 10 ウェブブラウザ121から通信仲介プログラム122を起動できる。

 ショップサーバ110とクライアントコンピュータ120は、インターネット140を介して接続される。

- 購入者携帯端末130には、前記クライアントコンピュータ120内の通信モジュール123とデータ通信が可能な通信モジュール131、個人識別情報13
- 15 3を含んだICカード132が備えられている。通信モジュール123、通信モジュール131の一例としては、Bluetoothや、IEEE802.11b用無線モジュールなどが好ましい。

- ICカード132は、ICチップが内蔵されたチップカードであり、演算機能、磁気カードよりも大容量のメモリ、そして高いセキュリティ機能を持つ。セキュ
- 20 リティ機能には、演算機能を使ってカード外部とのデータのやり取りを暗号化、復号化しデータの盗聴を防止する暗号機能や、耐タンパー性（外部からの物理的攻撃に抵抗し、解析されにくい特性）により、ICカードを分解し解析しようとすると、チップそのものが回路的に破壊されるような、偽造、変造、改ざん等を防止する機能がある。このようにして、ICカード132内の個人識別情報13
- 25 3そのものだけでなく、ICカード132と外部装置との個人識別情報133のデータのやり取りも保護されており、第三者に個人識別情報133が漏洩する可能性はPCよりも低い。

 個人識別情報133には、個人情報として、CA電子署名入り購入者携帯端末電子証明書と購入者携帯端末個人鍵が、決済情報として、クレジットカード決済

をするのに必要なクレジットカード情報が格納されている。なお例えば他に、個人情報として、住所、氏名、年齢、電話番号、血液型や、決済情報として、銀行口座番号等が格納されていてもよい。

- CA電子署名入り購入者携帯端末電子証明書は、購入者携帯端末130がCA
5 (Certification Authority、または認証局) から発行を受けた電子証明書にCA電子署名が付加されたものである。購入者携帯端末電子証明書には、購入者携帯端末公開鍵が含まれ、前記購入者携帯端末公開鍵が確かに購入者携帯端末本人のものであることはCAにより保証されている。

- 電子署名とは、公開鍵暗号化方式を利用しており、基になるデータを一定のアル
10 ゴリズム (ハッシュ関数) に従って変換したメッセージダイジェストを、署名者の個人鍵で暗号化したもので、この基になるデータと対にして利用される。ネットワークを介して受信した電子署名入りデータの信頼性は図2のようにして確認できる。

- 図2は、電子署名入りデータの信頼性確認の例を示す図である。本例は、CA
15 電子署名入り購入者携帯端末電子証明書を受信した場合である。受信側220では、CA電子署名222をCA公開鍵230で復号化することにより得られるメッセージダイジェスト225と、購入者携帯端末電子証明書221をハッシュ関数223で変換して得られるメッセージダイジェスト224を比較する。結果が同じであれば、伝送途中でデータが改ざんされておらず、またCA電子署名22
20 2が確かに購入者携帯端末電子証明書221に対してなされたものであることがわかる。CAの存在が信頼できることから、受信した購入者携帯端末電子証明書221の信頼性が確立する。なお、基になるデータは電子証明書に限られず、また署名者もCAに限られないが、その際は、図2の購入者携帯端末電子証明書、CA電子署名、CA公開鍵をそれぞれ対応するデータ、対応する署名者の電子署
25 名、対応する署名者の公開鍵として読みかえればよい。電子署名入り文書の信頼性確認は、本明細書においてしばしば行われるため、以後この確認手続きを「電子署名確認」と呼ぶ。

図3は、第一の実施例でのフローチャートである。第一の実施例は、購入者携帯端末電子証明書を用いて個人認証を行い、クレジットカード情報を用いて決済

認証を行うインターネットショッピングにおいて、通信仲介プログラムがショップサーバからの個人情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答されたCA電子署名入り購入者携帯端末電子証明書をショップサーバへ転送し、ショップサーバからの決済情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答されたクレジットカード情報をショップサーバへ転送し、それぞれの認証処理が行われる例である。

本実施例の前提として、ショップサーバはCA公開鍵301を取得済みであるとする。また、購入者携帯端末130内ICカードには、個人識別情報として、CA電子署名入り購入者携帯端末電子証明書302、クレジットカード情報303が格納されている。

まず購入者は、大画面で情報が得やすく操作性にも優れたクライアントコンピュータ120のウェブブラウザ121を使用して、インターネット140を介してショップサーバ110にアクセスし、ショップサーバ110に格納された販売者のホームページ111を閲覧し、商品の選択を行う(S1)。購入したい商品が決定したら、購入者は注文情報と購入意思をショップサーバへ送信する(S2)。ステップS2は例えば、事前に商品が選択されており、購入手続きに進むためにホームページに用意されたボタンをクリックすることで、それまでに選択された商品を購入する意思があると判定されることで実現されている。前記注文情報には、購入する商品と個数の情報が含まれる。

ショップサーバ110では、クライアントコンピュータ120へ購入手続き開始を通知する(S3)。ステップS3では、例えば購入開始を示す特別なHTMLタグが埋められたページが送信されたとする。前記購入手続き開始通知を受け、通信仲介プログラムが起動され、転送を開始する(S4)。ステップS4は、例えばウェブブラウザ121が前記購入開始を示す特別なHTMLタグを発見した際に通信仲介プログラム122を起動すればよい。次にショップサーバ110は、個人認証をするために、個人情報要求をクライアントコンピュータ120に送信する(S5)。通信仲介プログラム122は、前記個人情報要求を、通信モジュール123を介して購入者携帯端末130へ転送する(S6)。前記個人情報要求に対し、購入者携帯端末130では、ICカード132が格納された個人識別

情報133からCA電子署名入り購入者携帯端末電子証明書302を応答し、前記CA電子署名入り購入者携帯端末電子証明書は通信モジュール131を介して、クライアントコンピュータ120へ送信される(S7)。通信仲介プログラム122は、クライアントコンピュータのハードディスクにCA電子署名入り購入者携帯端末電子証明書302を書き込むことなく、ショップサーバ110へ前記CA電子署名入り購入者携帯端末電子証明書を転送する(S8)。ショップサーバ110では、CA公開鍵301を使用して、CA電子署名入り購入者携帯端末電子証明書302の電子署名確認を行う(S9)。電子署名確認の手順は、図2に述べられている。ステップS9にて、購入者携帯端末電子証明書の信頼性が確立すると、個人認証は完了する。

ステップS9にて個人認証が成功すると、続いてショップサーバ110は、クライアントコンピュータ120に対して、決済情報を要求する(S10)。通信仲介プログラム122は、前記決済情報要求を購入者携帯端末130へ転送する(S11)。前記決済情報要求に対し、購入者携帯端末130内ICカード132はクレジットカード情報303を応答し、前記クレジットカード情報は通信モジュール131を介して、クライアントコンピュータ120へ送信される(S12)。通信仲介プログラム122は、クライアントコンピュータのハードディスクにクレジットカード情報303を書き込むことなく、前記クレジットカード情報をショップサーバへ転送する(S13)。ショップサーバでは、クレジットカード情報303を基に与信審査を行い、決済認証を完了する(S14)。続いて、図示はしないが、決済認証結果による商品の出荷処理を経て、第一の実施例は終了する。

なおステップS12でのクレジットカード情報303の応答は、ショップサーバ以外の第三者に盗聴されないよう暗号化を施すことが望ましい。例えば、購入者携帯端末130が、ショップサーバ公開鍵を取得していれば、当該ショップサーバ公開鍵を用いて暗号化すればよい。また本実施例では、個人認証と決済認証を分けて実施している例であるが、個人情報要求と決済情報要求が一度に行われることもある。その場合、ステップS7において、購入者携帯端末130内のICカード132がCA電子署名入り購入者携帯端末電子証明書302とクレジッ

トカード情報 303 を同時に応答すればよい。

本実施例により、商品の選択には画面の大きなクライアントコンピュータを使用しながら、購入者携帯端末内 IC カードに格納された、第三者に漏洩しにくい個人識別情報を使用して、個人認証や決済認証を完了することができる。したがって、クライアントコンピュータのハードディスクに個人識別情報を残すことなく、インターネットショッピングを行うことができ、インターネットショッピングをしやすい環境とハードディスクからの個人識別情報の読み出しによる成りすまし防止を両立することができる。

図 4、5 は、第二の実施例でのフローチャートである。図 4 における携帯端末 130、クライアントコンピュータ 120、ショップサーバ 110 のフロー下端、407、408、409 はそれぞれ図 5 の対応するフローの上端と一続きであり、したがって二図を合わせて説明する。第二の実施例は、購入者携帯電子証明書を用いて個人認証を行い、クレジットカード情報を用いて決済認証を行うインターネットショッピングにおいて、通信仲介プログラムがショップサーバからの個人情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答された CA 署名入り購入者電子署名をショップサーバへ転送し、ショップサーバからの決済情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答された共通鍵暗号化方式を用いて暗号化された決済情報をショップサーバへ転送し、それぞれ認証処理が行われる例である。

本実施例の前提として、購入者携帯端末 130 内 IC カードには、個人識別情報として、CA 電子署名入り購入者携帯端末電子証明書 302、クレジットカード情報 303 が、ショップサーバ 110 は CA 電子署名入りショップサーバ電子証明書 401 を得ている。また購入者携帯端末、ショップサーバはともに CA 公開鍵 301 を取得済みである。

図 4 において、まず購入者は、大画面で情報が得やすく操作性にも優れたクライアントコンピュータ 120 のウェブブラウザ 121 を使用して、インターネット 140 を介してショップサーバ 110 にアクセスし、ショップサーバ 110 に格納された販売者のホームページ 111 を閲覧し、商品の選択を行う (S1)。購入したい商品が決定したら、購入者は注文情報 402 と購入の意思をショップ

サーバへ送信する（S2）。ステップS2は例えば、購入手続きに進むためにホームページに用意されたボタンをクリックすることで、それまでに選択された商品を購入する意思があると判定されることで実現されている。注文情報402は、購入する商品と個数の情報である。

- 5 ショップサーバ110では、クライアントコンピュータ120へ購入手続き開始を通知する（S3）。ステップS3では、例えば購入開始を示す特別なHTMLタグが埋められたページが送信されるとする。前記購入手続き開始通知を受け、通信仲介プログラムが起動され、転送を開始する（S4）。ステップS4は、例えばウェブブラウザ121が前記購入開始を示す特別なHTMLタグを発見した
- 10 際に通信仲介プログラム122を起動すればよい。

- ショップサーバ110はクライアントコンピュータ120へ個人情報要求とCA電子署名入りショップサーバ電子証明書401を送信する（S15）。通信仲介プログラム122は購入者携帯端末130へ前記個人情報要求及びCA電子署名入りショップサーバ電子証明書401を転送する（S16）。購入者携帯端末
- 15 130内ICカード132は、CA公開鍵301を使用して、CA電子署名入りショップサーバ電子証明書401の電子署名確認を行う（S17）。ステップS17にて、ショップサーバ電子証明書の信頼性が確立すると、ショップサーバ認証は完了する。

- ステップS17でショップサーバ認証が済むと、前記個人情報要求に対し購入
- 20 者携帯端末130内のICカード132はCA電子署名入り購入者携帯端末電子証明書302を応答し、前記CA電子署名入り購入者携帯端末電子証明書はクライアントコンピュータ120へ送信される（S18）。通信仲介プログラム122は、クライアントコンピュータ120のハードディスクにCA電子署名入り購入者携帯端末電子証明書302を書き込むことなく、ショップサーバ110へ前
- 25 記CA電子署名入り購入者携帯端末電子証明書を転送する（S19）。ショップサーバ110は、CA電子署名入り購入者携帯端末電子証明書302の電子署名確認を行う（S20）。ステップS20にて、購入者携帯端末電子証明書の信頼性が確立すると、個人認証が完了する。ステップS20で購入者携帯端末電子証明書の信頼性が確立したので、後の使用のため前記購入者携帯端末電子証明書に

含まれる購入者携帯端末公開鍵403を保存する。

次にショップサーバ110は、共通鍵暗号化方式で以降の通信を暗号化するために共通鍵に相当する、セッション鍵404を作成する(S21)。ショップサーバ110は、購入者携帯端末公開鍵403でセッション鍵404および注文情報402を暗号化し、クライアントコンピュータへ暗号化されたセッション鍵405と暗号化された注文情報406を送信する(S22)。購入者携帯端末公開鍵403で暗号化することで、セッション鍵404および注文情報402は購入者携帯端末個人鍵を持っていないと取り出せず、事実上それは購入者携帯端末でしか復号化できない。通信仲介プログラム122は、購入者携帯端末130へ暗号化されたセッション鍵405と暗号化された注文情報406を転送する(S23)。購入者携帯端末130内ICカードは、購入者携帯端末の個人鍵を使用して暗号化されたセッション鍵405と暗号化された注文情報406を復号化し、セッション鍵404、注文情報402を取り出す(S24)。

これより図5である。続いて、購入者携帯端末130内ICカード132は、購入者に購入商品をクライアントコンピュータ上で確認させるために、非転送フラグ付きで、注文情報402を応答し、前記注文情報は、通信モジュール131を介しクライアントコンピュータ120へ送信される(S25)。この非転送フラグは、仲介プログラムに転送させたくないデータがある場合に使用される。非転送フラグは例えば、非転送フラグを示す特殊なHTMLタグが埋められたページが送信されることで実現される。通信仲介プログラム122は非転送フラグを発見し、注文情報402をウェブブラウザ121に表示させ、購入者に前記注文情報を最終確認させ、最終確認結果をブラウザ121から受け取ると、購入がキャンセルされたのでなければ、決済情報要求を購入者携帯端末130に送信する(S26)。

購入者携帯端末130内のICカード132は、前記決済情報要求に対し、クレジットカード情報303をセッション鍵404で暗号化した暗号化されたクレジットカード情報501を応答し、前記暗号化されたクレジットカード情報は、クライアントコンピュータへ送信される(S27)。通信仲介プログラム122は、クライアントコンピュータ120のハードディスクに暗号化されたクレジッ

トカード情報501を書き込むことなく、ショップサーバ110へ前記暗号化されたクレジットカード情報を転送する(S28)。ショップサーバ110では、暗号化されたクレジットカード情報501が復号化され、クレジットカード情報303が取り出される(S29)。そして、クレジットカードの与信審査をもつて決済認証が完了する(S30)。その後、図示はしないが、決済認証結果による商品の出荷処理を経て、第二の実施例は終了する。

本実施例により、商品の選択には画面の大きなクライアントコンピュータを使用しながら、購入者携帯端末内ICカードに格納された、第三者に漏洩しにくい個人識別情報を使用し、クライアントコンピュータに個人識別情報を残すことなく、さらにショップサーバと購入者携帯端末間の通信をセッション鍵で暗号化し、個人認証や決済認証を完了することができる。したがって、インターネットショッピングをしやすい環境を保ちつつ、クライアントコンピュータのハードディスクからの個人識別情報の読み出しによる成りすましを防止するだけでなく、購入者携帯端末、クライアントコンピュータ、ショップサーバ間の通信盗聴による個人識別情報漏洩による成りすましも防止することができる。

図6、7、8、9は、第三の実施例でのフローチャートである。第二の実施例における図4と図5の関係と同じく、図6のフロー下端と図7のフロー上端、図7のフロー下端と図8のフロー上端、図8のフロー下端と図9のフロー上端は一続きになっており、したがって四図を合わせて説明する。第三の実施例では、SET(Secure Electronic Transaction)という既存のクレジットカード決済の標準規格として開発された仕組みに本発明を適用した例である。第三の実施例は、購入者携帯端末電子証明書を用いて個人認証を行い、クレジットカード情報を用いて決済認証を行うインターネットショッピングにおいて、通信仲介プログラムがショップサーバからの個人情報要求を購入者携帯端末に転送し、購入者携帯端末から応答されたCAの電子署名入り購入者電子証明書をショップサーバへ転送し、ショップサーバからの決済情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答されたカード会社サーバ公開鍵で暗号化されたクレジットカード情報含むデータをショップサーバに転送し、それぞれ認証処理が行われる例である。

本実施例の前提として、購入者携帯端末130は、ウォレットと呼ばれる、通常SETにおいては購入者のPCで実行されるソフトウェアの機能进行处理することができる。また購入者携帯端末130はCA電子署名入り購入者携帯端末電子証明書302を、ショップサーバ110はCA電子署名入りショップサーバ電子証明書401を、カード会社サーバ150はCA電子署名入りカード会社サーバ電子証明書601を得ている。また購入者携帯端末130、ショップサーバ110、カード会社サーバ150はともにCA公開鍵301を取得済みである。

あらかじめカード会社サーバは、ショップサーバへCA電子署名入りカード会社サーバ電子証明書410を送信する(S31)。

10 図6において、まず購入者は、大画面で情報が得やすく操作性にも優れたクライアントコンピュータ120のウェブブラウザ121を使用して、インターネット140を介してショップサーバ110にアクセスし、ショップサーバ110に格納された販売者のホームページ111を閲覧し、商品の選択を行う(S1)。

15 購入したい商品が決定したら、購入者は注文情報402と購入の意思をショップサーバへ送信する(S2)。ステップS2は例えば、購入手続きに進むためにホームページに用意されたボタンをクリックすることで、それまでに選択された商品を購入する意思があると判定されることで実現されている。注文情報402は、購入する商品と個数の情報である。

ショップサーバ110では、クライアントコンピュータ120へ購入手続き開始を通知する(S3)。ステップS3では、例えば購入開始を示す特別なHTMLタグが埋められたページが送信されたとする。前記購入手続き開始通知を受け、通信仲介プログラムが起動され、転送を開始する(S4)。

ショップサーバ110は、クライアントコンピュータ120へCA電子署名入りカード会社サーバ電子証明書601、CA電子署名入りショップサーバ電子証明書401、注文情報402を送信する(S32)。通信仲介プログラム122は、購入者携帯端末130へCA電子署名入りカード会社サーバ電子証明書601、CA電子署名入りショップサーバ電子証明書401、注文情報402を転送する(S33)。

購入者携帯端末130内ICカード132は、CA公開鍵301を使用して、

CA電子署名入りショップサーバ電子証明書401の電子署名確認を行い、ショップサーバ認証を行う(S34)。認証が成功したら、ショップサーバ電子証明書に含まれるショップサーバ公開鍵602を保存する。続いてCA公開鍵301を使用して、CA電子署名入りカード会社サーバ電子証明書601の電子署名確認も行い、カード会社サーバ認証を行う(S35)。認証が成功したら、カード会社サーバ電子証明書に含まれるカード会社サーバ公開鍵603を保存する。次に購入者携帯端末130内ICカード132は注文情報403を基データとして購入者携帯端末電子署名を作成し、購入者携帯端末電子署名入り注文情報604を作成する(S36)。前記購入者携帯端末電子署名はこの注文が確かに購入者によってなされたことを確定するためのもので、これにより購入者は言い逃れができない。

これより図7である。さらに購入者携帯端末130内のICカード132は、クレジットカード情報303と注文情報402から作成したメッセージダイジェストをまとめたデータを決済情報とし、カード会社サーバ公開鍵603で暗号化し、暗号化された決済情報701を作成する(S37)。これにより、クレジットカード情報303はクレジットカード会社の個人鍵でのみ復号化でき、ショップにおいて盗み見られることはない。こうしてCA電子署名入り購入者携帯端末電子証明書302、購入者携帯端末電子署名入り注文情報604、暗号化された決済情報701が、クライアントコンピュータ120へ送信される(S38)。

通信仲介プログラム122は、ショップサーバ110へCA電子署名入り購入者携帯端末電子証明書302、購入者携帯端末電子署名入り注文情報604、クレジットカード会社サーバ公開鍵にて暗号化された決済情報701を転送する(S39)。

ショップサーバ110では、CA電子署名入り購入者携帯端末電子証明書302の電子署名確認を行い、個人認証を行う(S40)。認証に成功したら、購入者携帯端末公開鍵403を保存する。次に購入者携帯端末電子署名入り注文情報604の電子署名確認を行う(S41)。比較の結果が同じであれば、注文情報が信頼でき、ショップは購入者に提供すべき商品名や個数などがわかる。ここで、注文に対して購入者とショップの同意が取れたことの証しとして、ショップサー

パは、注文情報403から作成したメッセージダイジェストを基データとしてショップサーバ電子署名を作成し、ショップサーバ電子署名入りメッセージダイジェスト702を作成する(S42)。そして、ショップサーバ110はカード会社サーバ150へ、CA電子署名入り購入者携帯端末電子証明書302、CA電子署名入りショップサーバ電子証明書401、ショップサーバ電子署名入りメッセージダイジェスト702、カード会社サーバ公開鍵603で暗号化された決済情報701を送信する(S43)。注文情報を直接送るのではなく、メッセージダイジェストを送ることによって、カード会社サーバには注文の内容は伝わらず、単に合計金額と、購入者とショップが注文に対して同意が取れているという事実だけが伝わることになる。

カード会社サーバ150では、CA電子署名入りショップサーバ電子証明書401の電子署名確認を行い、ショップサーバ認証を行う(S44)。認証が成功したら、ショップサーバ電子証明書に含まれるショップサーバ公開鍵602を保存する。

これより図8である。続いてカード会社サーバ150は、CA電子署名入り購入者携帯端末電子証明書302の電子署名確認を行い、個人認証を行う(S45)。認証が成功したら、購入者携帯端末電子証明書に含まれる購入者携帯端末公開鍵403を保存する。次にカード会社サーバ個人鍵で暗号化された決済情報701を復号する(S46)。決済情報からクレジットカード情報を取り出し、与信審査を行って決済認証を行う(S47)。さらに、ショップサーバ電子署名入りメッセージダイジェスト702の電子署名確認を行い、購入者とショップが注文に同意しているかを確認する(S48)。カード会社サーバ150は直接の注文情報403は把握できないが、販売者がステップS25にて購入者からの注文情報403の内容を確認したことを確認することができる。次に、送信されたメッセージダイジェスト506と決済情報304を復号化した際に得られる注文情報403から作成したメッセージダイジェストを比較する(S49)。これは、決済される金額が注文情報403に基づくものであるかを確認するためである。比較の結果が同じであれば、ショップが請求した金額が確かに購入者の注文情報403に基づくものであると確認できる。ショップに審査結果を通知するために、カ

ード会社サーバ電子署名入り審査結果801を作成する(S50)。カード会社サーバ150は、ショップサーバ110へ、カード会社サーバ電子署名入り審査結果801、カード会社サーバ公開鍵603で暗号化された決済情報701を送信する(S51)。

- 5 これより図9である。ショップサーバ110では、カード会社サーバ電子署名入り審査結果801の電子署名確認を行い、審査結果をもって、決済認証を完了する(S52)。購入者に伝えるため、審査結果を基データとしてショップサーバ電子署名を作成し、ショップサーバ電子署名入り審査結果901を作成する(S53)。クライアントコンピュータ120へ、ショップサーバ電子署名入り審査結果901、カード会社サーバ公開鍵603で暗号化された決済情報701を送信する(S54)。

通信仲介プログラム122は、購入者携帯端末130へ、ショップサーバ電子署名入り審査結果901、暗号化された決済情報701を転送する(S55)。

- 15 購入者携帯端末130内ICカード132は、ショップサーバ電子署名404入り審査結果の電子署名確認を行い、信頼性を確認した後、審査結果を確認する(S56)。このとき、購入者携帯端末からクライアントコンピュータへすべての処理の終了が通知され、例えばその通知がブラウザに表示されてもよい。これにより第三の実施例は終了する。

- 本実施例により、商品の選択には画面の大きなクライアントコンピュータを使用しながら、購入者携帯端末内ICカードに格納された、第三者に漏洩しにくい個人識別情報を使用し、さらにSETの仕組みを既存のまま利用して、個人認証や決済認証を完了することができる。したがって、インターネットショッピングをしやすい環境を保ちつつ、クライアントコンピュータのハードディスクからの個人識別情報の読み出しによる「成りすまし」を防止するだけでなく、購入者携
- 25 帯端末、クライアントコンピュータ、ショップサーバ、カード会社サーバ間の通信盗聴による個人識別情報漏洩による「成りすまし」も防止することができ、さらにSETの設備が整備されていれば、そのまま用いることができ、過去の設備投資を無駄にしなくて済むメリットがある。

以上述べてきた本発明の実施例は、ショップサーバで行われる購入処理に伴う

認証処理に限定されるものではなく、他の処理に伴う認証処理にも適用が可能である。

〔産業上の利用の可能性〕

- 5 以上説明したように本発明によれば、インターネットショッピングにおいて、商品の選択には画面の大きなクライアントコンピュータを使用しながら、第三者によってデータが読み出される可能性のあるクライアントコンピュータのハードディスクに、購入者の個人識別情報を格納することなく、個人認証、決済認証が完了する環境を提供することができ、なりすましを防止することができる。さら
- 10 に、購入者携帯端末内のＩＣカードの持つ暗号化機能を利用すれば、サーバと購入者携帯端末間の通信データも保護でき、個人識別情報が盗聴されることによる成りすましも防止可能である。

請求の範囲

1. サーバにコンピュータネットワークを介して接続可能なクライアントコンピュータに、個人識別情報が格納された携帯端末と共働して、個人識別処理を実行させるプログラムにおいて、

5 前記個人識別処理は、
 前記サーバからの個人識別情報要求信号に応答して、当該個人識別情報要求信号を前記携帯端末に転送する手順と、
 前記携帯端末に格納される前記個人識別情報であって、前記携帯端末が前記個人識別情報要求信号に
10 前記個人識別情報要求信号に
 前記クライアントコンピュータに送信する前記個人識別情報を、前記サーバに転送する手順とを有することを特徴とするプログラム。
2. 請求項 1 において、

 前記個人識別処理は、
 受信したデータに非転送フラグが含まれている時は、当該受信データを
15 転送しない手順を有することを特徴とするプログラム。
3. 請求項 1 において、

 前記個人識別処理に先立ち、
 前記サーバに接続して前記クライアントコンピュータにインストールされているブラウザによる電子商取引のセッション中に、前記ショ
20 プサーバからの指令に対応する起動命令に
 前記クライアントコンピュータに実行させることを特徴とするプログラム。
4. 請求項 1 において、

 前記個人識別情報は、前記電子商取引を行う個人を特定する個人情報と、
 当該電子商取引を行う個人の決済情報のいずれか一方を少なくとも有する
25 ことを特徴とするプログラム。
5. 請求項 3 において、

 前記個人情報は、前記携帯端末の個人電子証明書と当該個人電子証明書の認証局の電子署名とを有することを特徴とするプログラム。
6. 請求項 3 において、

前記決済情報は、クレジットカードIDまたは金融機関の引落口座IDのいずれか一つを有することを特徴とするプログラム。

7. 請求項1において、

5 前記携帯端末が前記個人識別情報要求信号に応答して前記クライアントコンピュータに送信する前記個人識別情報は、所定の暗号鍵に従って暗号化されていることを特徴とするプログラム。

8. 請求項6において、

10 前記所定の暗号鍵は、前記サーバ若しくはクレジットカード会社の公開鍵、または前記電子商取引のセッション時に作成されたセッション鍵のいずれかであることを特徴とするプログラム。

9. サーバにコンピュータネットワークを介して接続可能なクライアントコンピュータであって、

前記サーバからの個人識別情報要求信号に応答して、当該個人識別情報要求信号を個人識別情報が格納された携帯端末に転送する手段と、

15 前記携帯端末に格納される前記個人識別情報であって、前記携帯端末が前記個人識別情報要求信号に応答して当該クライアントコンピュータに送信する前記個人識別情報を、前記サーバに転送する手段と、

を有することを特徴とする、前記携帯端末と共働する個人識別処理を行うクライアントコンピュータ。

20

図1

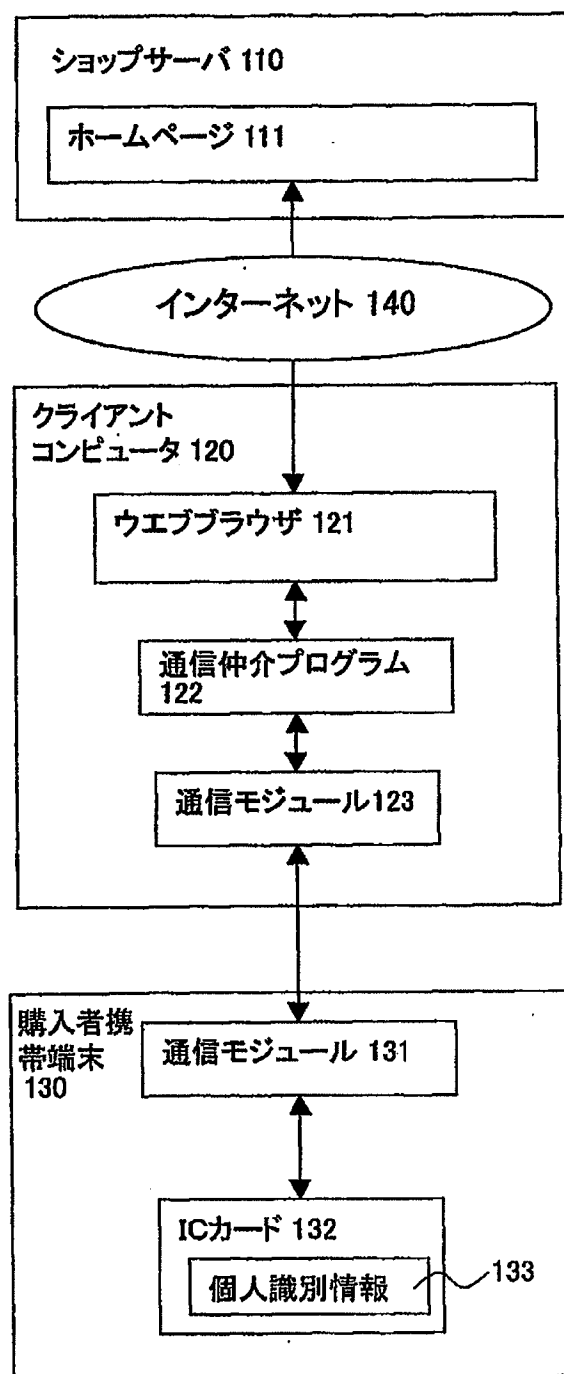


图2

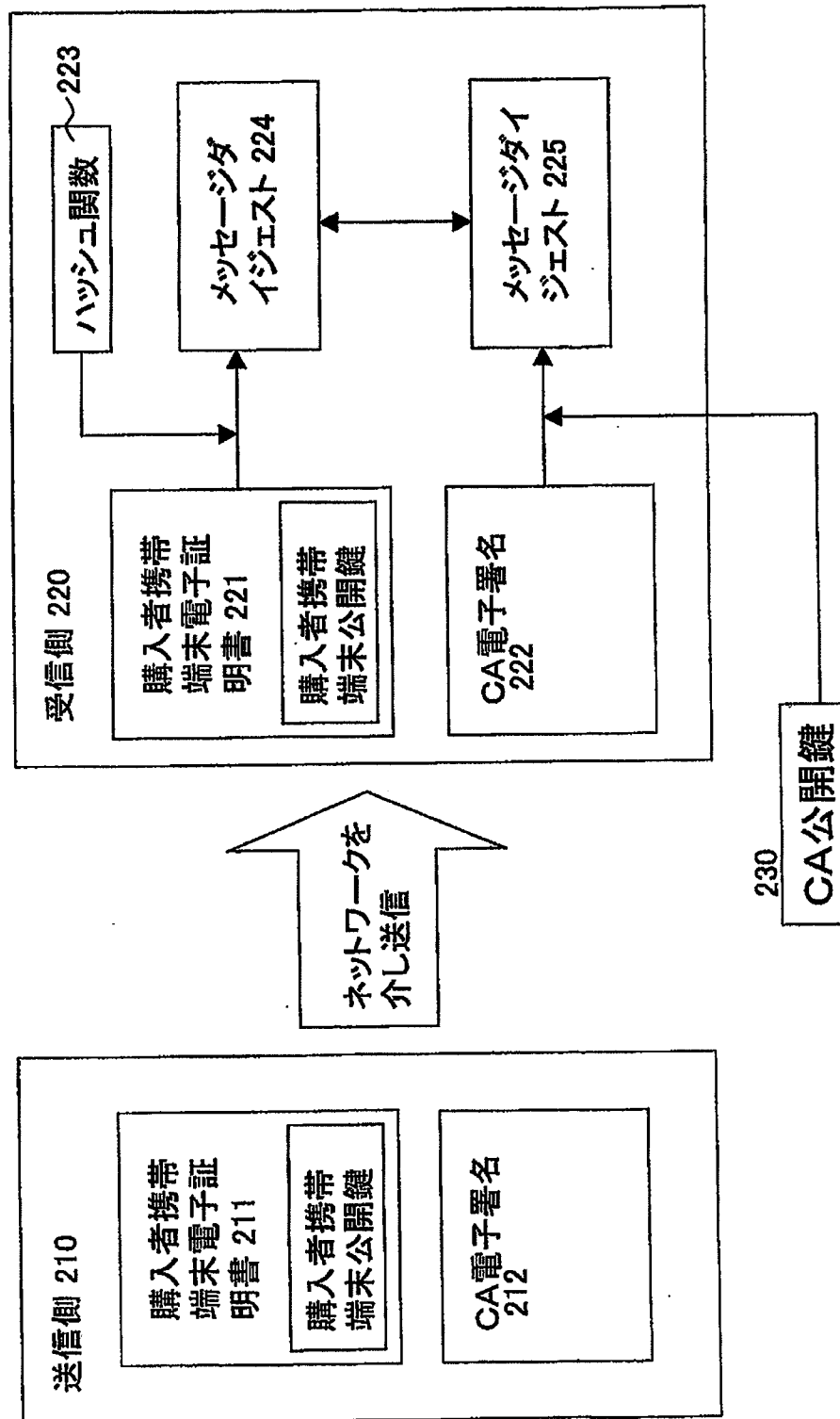


図3

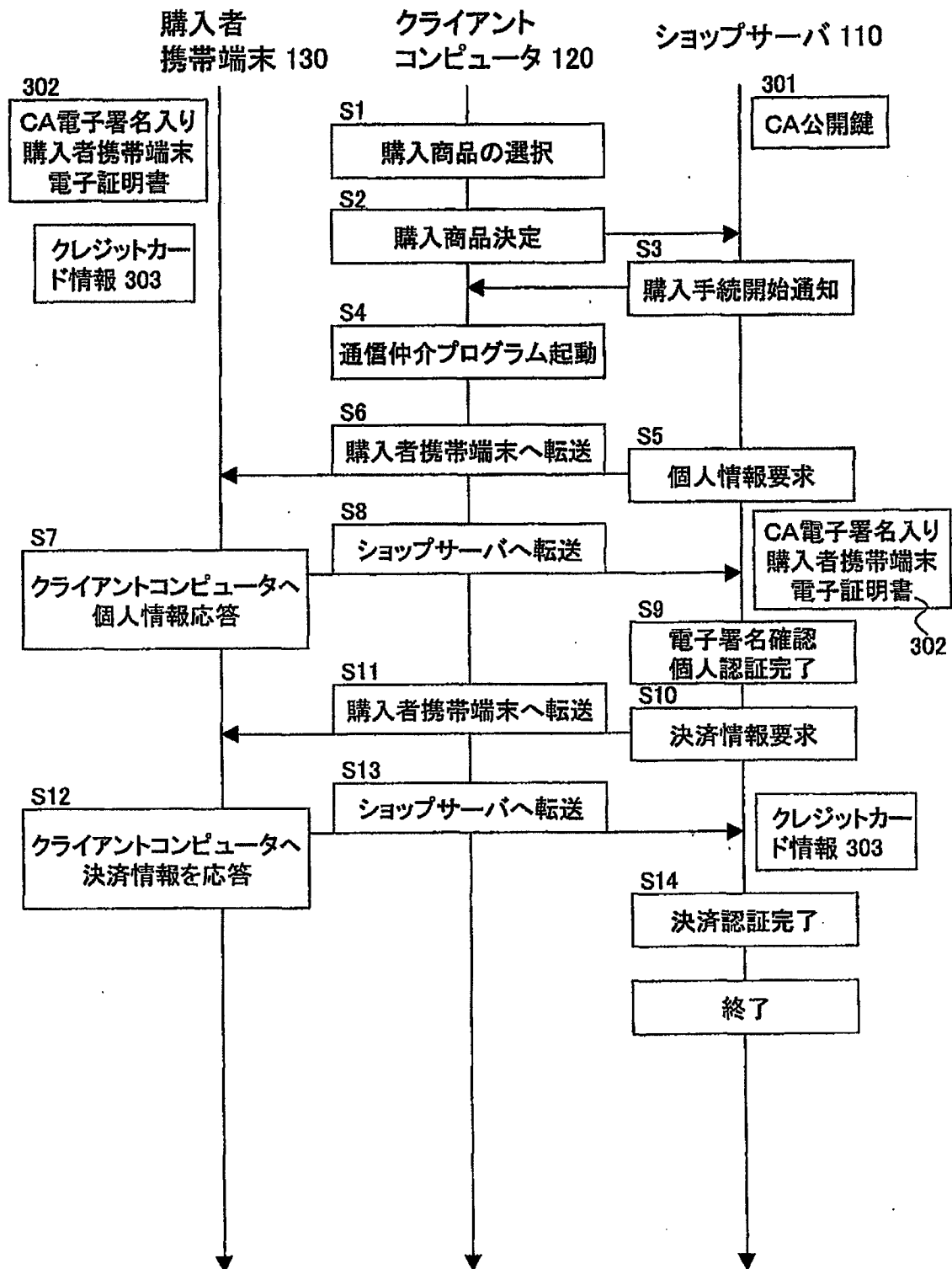


図4

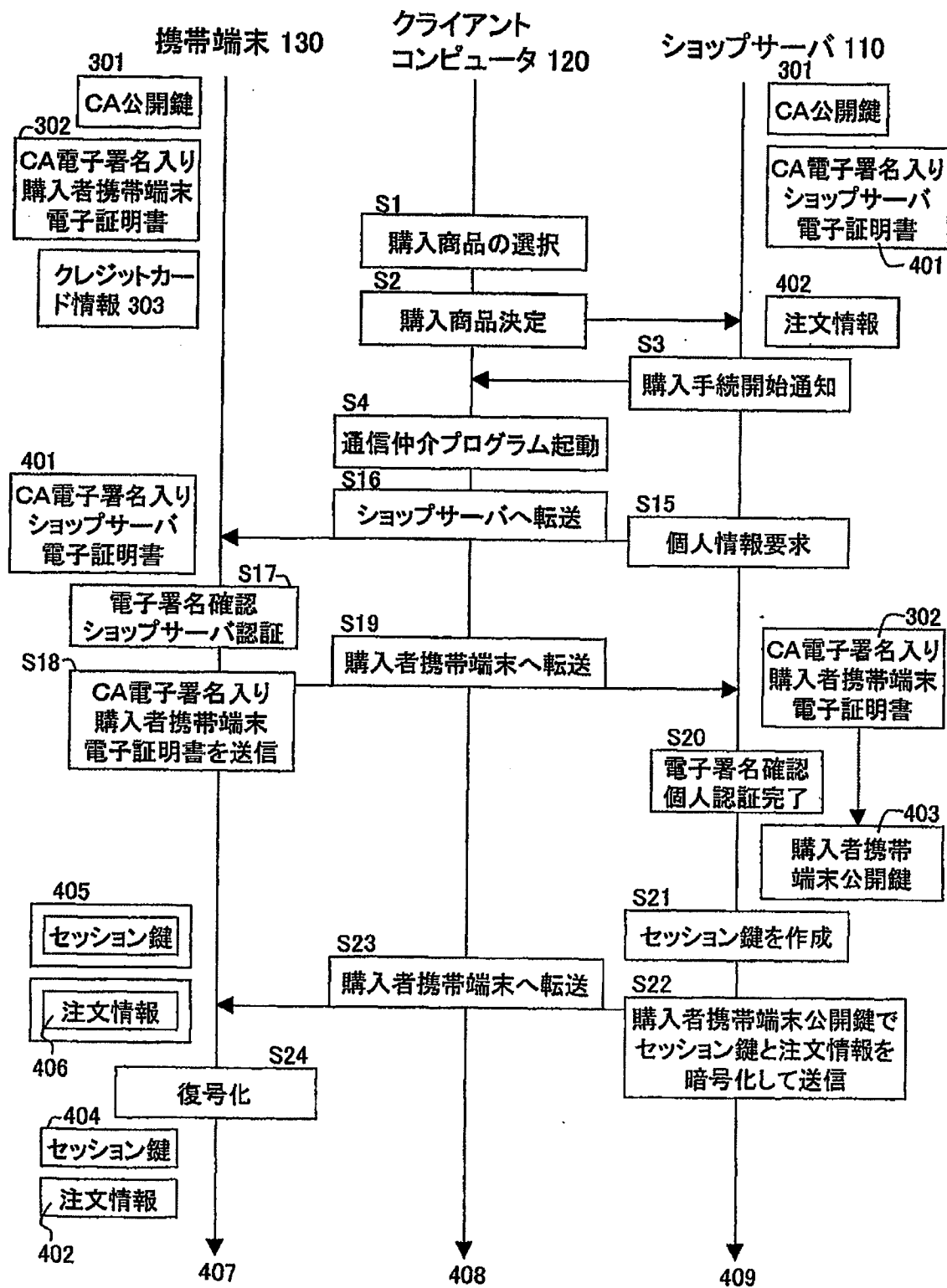


図5

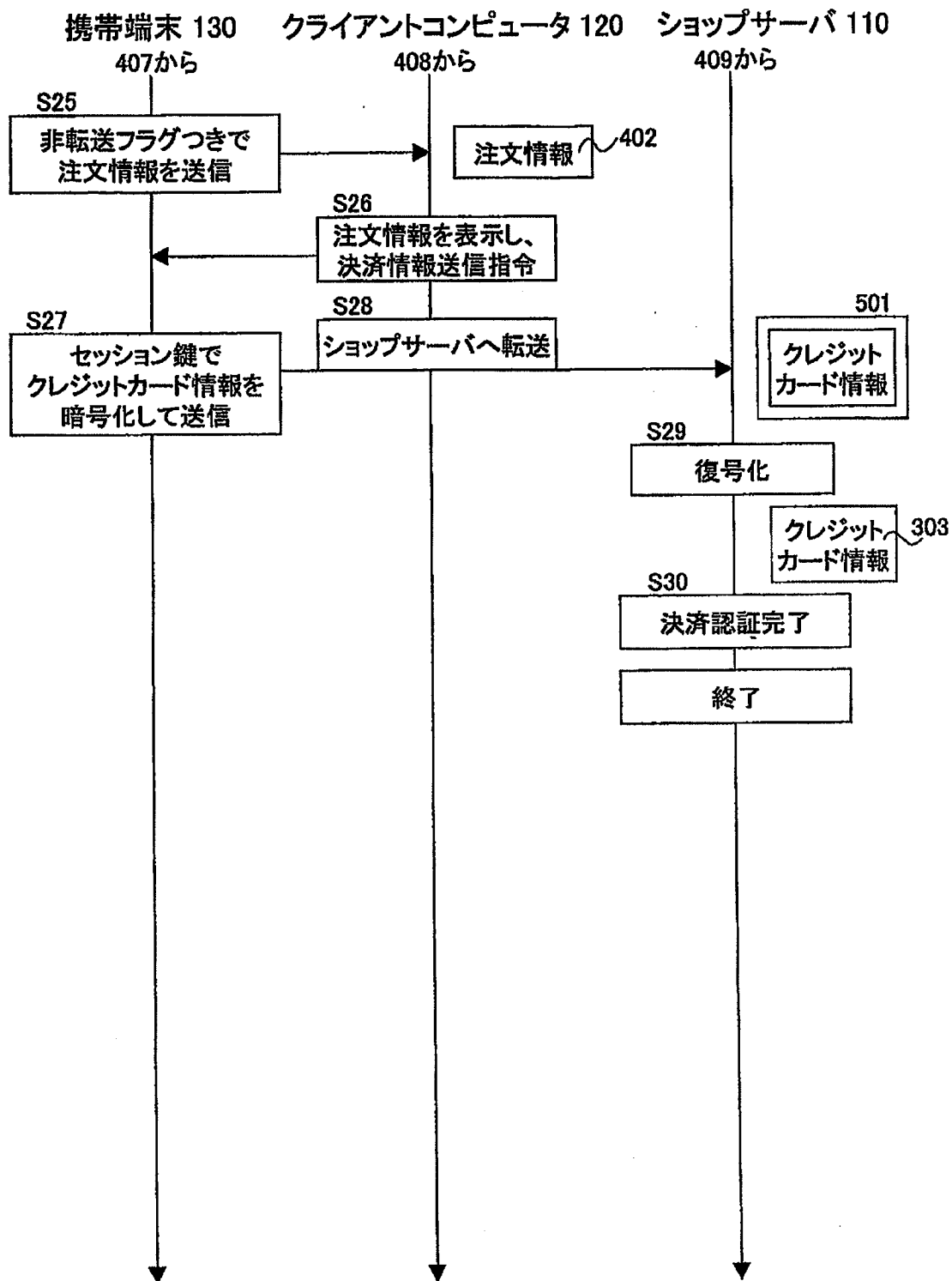


図6

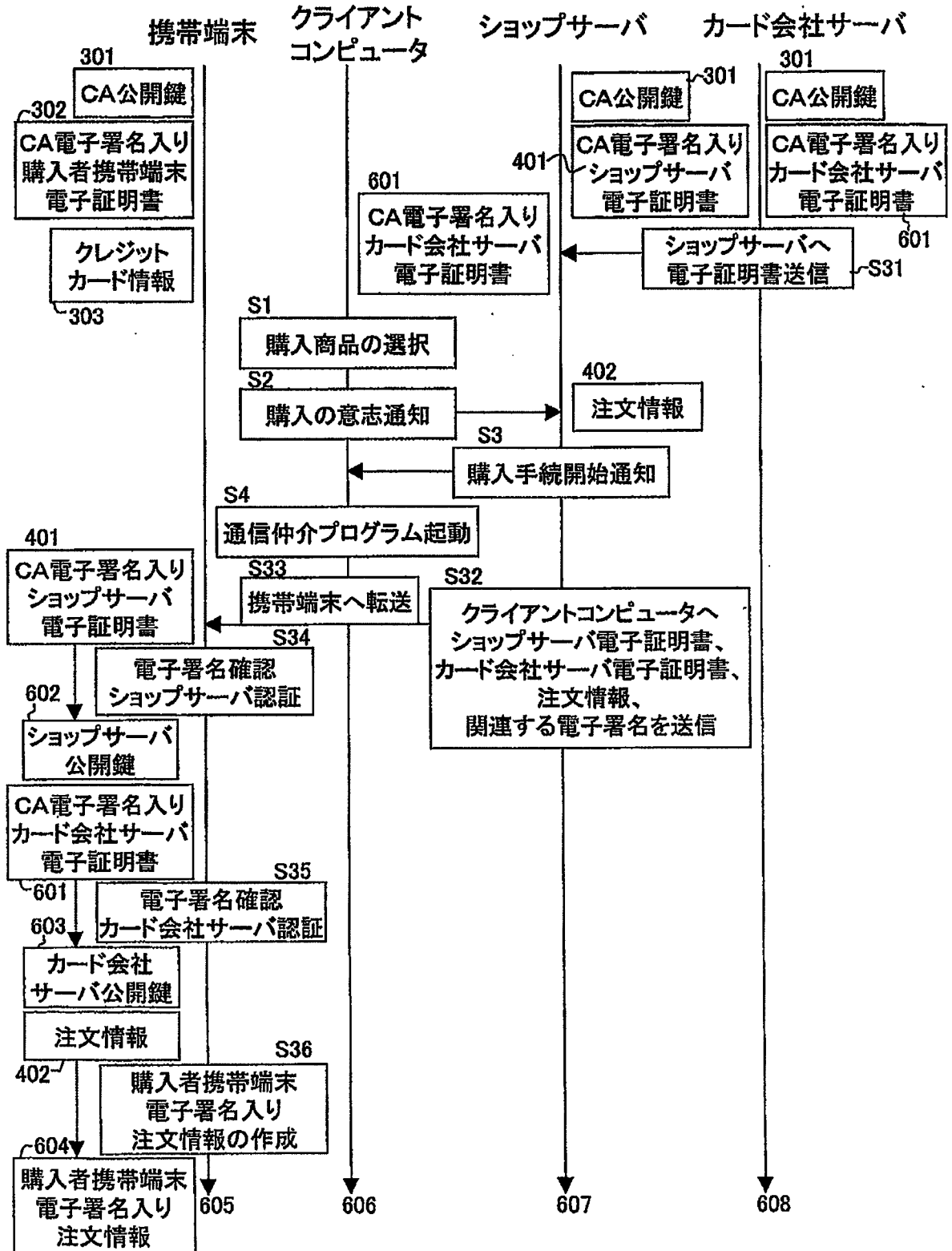


図7

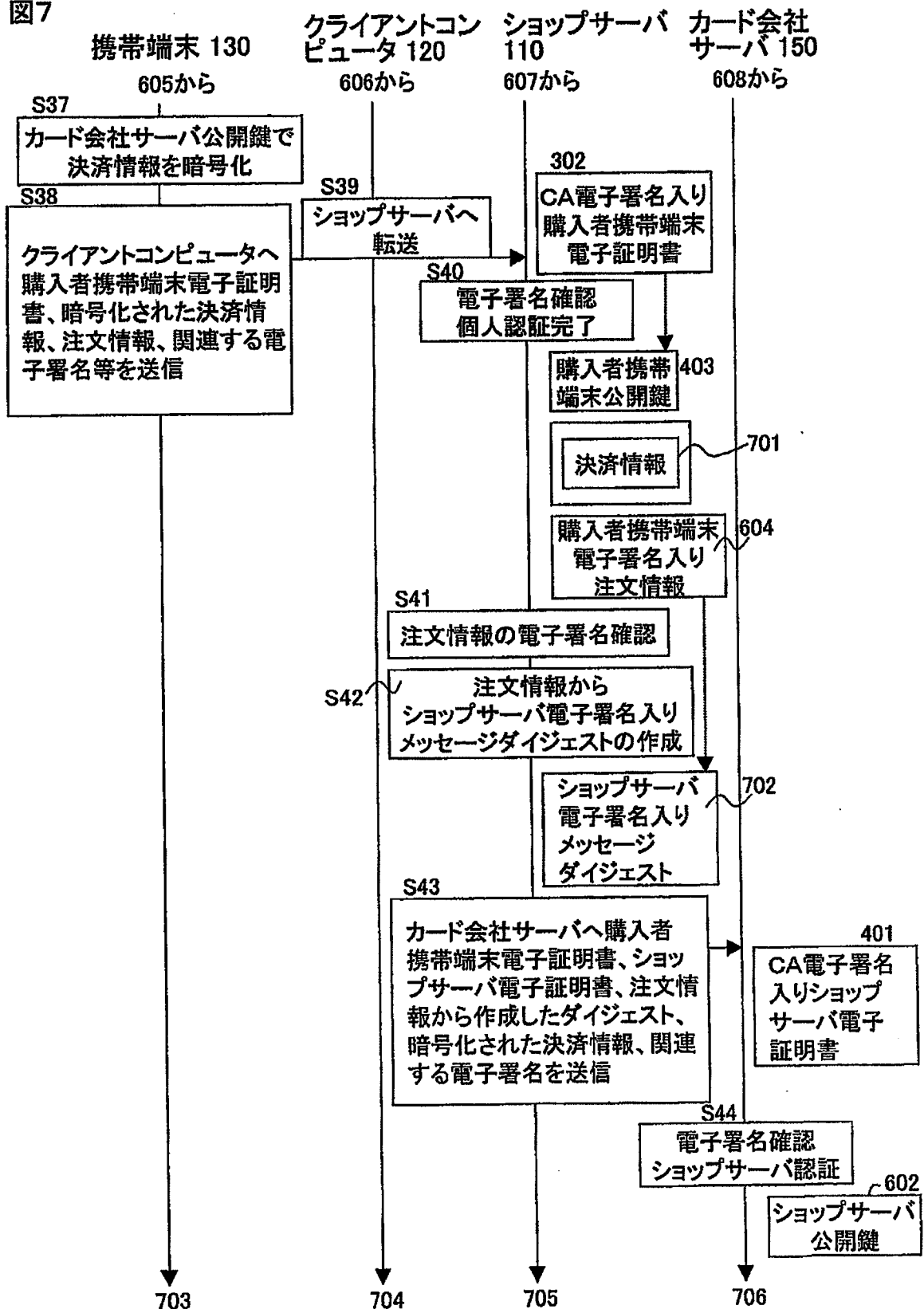


図8

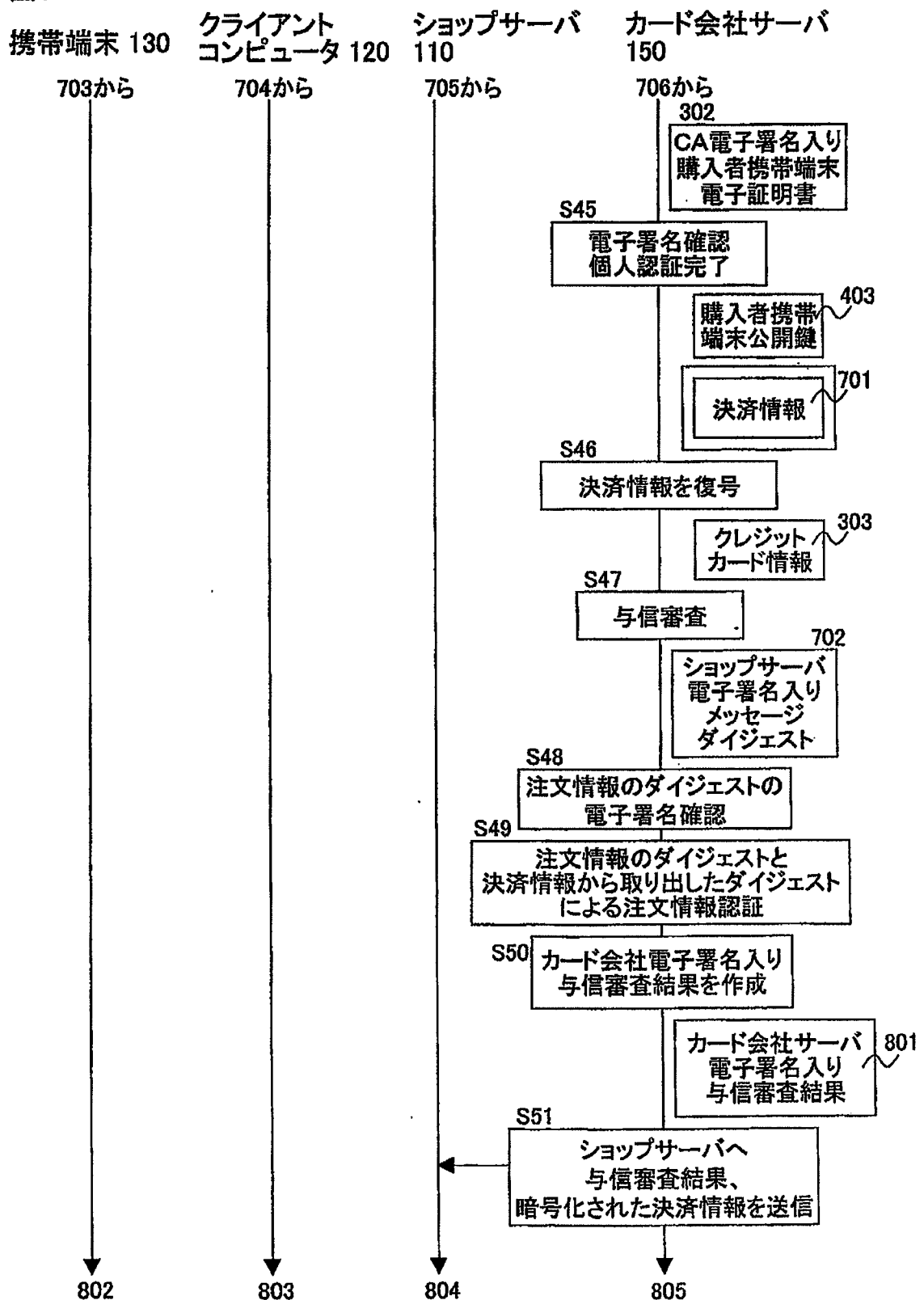
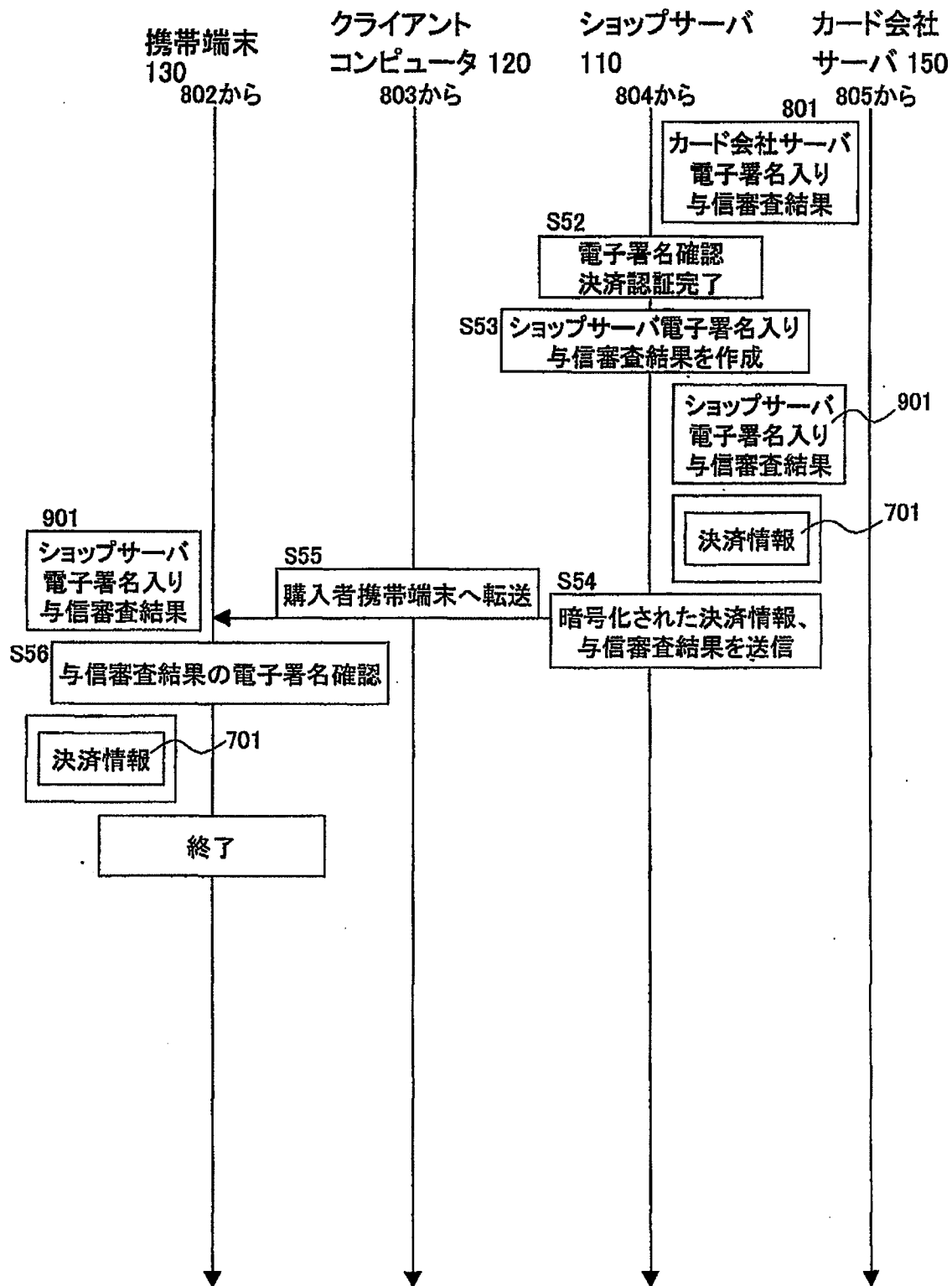


図9



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/05582

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F17/60; G06K17/00, G06K19/07

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6182900 B1 (Siemens Nixdorf Informationssysteme AG.), 06 February, 2001 (06.02.01), Column 5, lines 34 to 50 & AU 63910/98 A & DE 19710249 A1 & EP 0970447 A2 & JP 2001-515621 A & WO 98/40851 A2	1-9
Y	JP 2000-138672 A (NTT Data Corp.), 16 May, 2000 (16.05.00), Fig. 3 (Family: none)	1-9
Y	EP 1030272 A2 (Matsushita Electric Industrial Co., Ltd.), 23 August, 2000 (23.08.00), Fig. 6 & JP 2000-306003 A	1-9

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
10 September, 2002 (10.09.02)Date of mailing of the international search report
08 October, 2002 (08.10.02)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/05582

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-083243 A (Dainippon Printing Co., Ltd.), 22 March, 2002 (22.03.02), Fig. 1 (Family: none)	1-9

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ G06F17/60; G06K17/00, G06K19/07

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996 年
日本国公開実用新案公報	1971-2002 年
日本国登録実用新案公報	1994-2002 年
日本国実用新案登録公報	1996-2002 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	US 6182900 B1 (SIEMENS NIXDORF INFORMATIONSSYSTEME AG) 2001.02.06 コラム5, 34-50 行 & AU 63910/98 A & DE 19710249 A1 & EP 0970447 A2 & JP 2001-515621 A & WO 98/40851 A2	1-9

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

10.09.02

国際調査報告の発送日

03.10.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

阿波 進

5 L

9 1 6 8

電話番号 03-3581-1101 内線 3561

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2000-138672 A (株式会社エヌ・ティ・ティ・データ) 2000.05.16 図 3 (ファミリーなし)	1-9
Y	EP 1030272 A2 (MATSUSHITA ELECTRIC INDUSTRY CO., LTD.) 2000.08.23 図 6 & JP 2000-306003 A	1-9
Y	JP 2002-083243 A (大日本印刷株式会社) 2002.03.22 図 1 (ファミリーなし)	1-9